

SYSTEM AND METHOD FOR PROVIDING TRUSTED BROWSER VERIFICATION

BACKGROUND OF THE INVENTION

5 The world of electronic commerce has created new challenges to establishing relationships between contracting parties. One of those challenges springs from the fact that the parties to the transaction can not see or hear each other, and can not otherwise easily confirm each other's identity and authority to act.

One remedy for this problem is to provide each contracting party with a private key
10 for signing transmitted messages. The signing party makes available an associated public key that decrypts messages signed with the party's private key, and thus enables a receiving party to confirm the identity of the sender.

But the sender's public key may not be known *a priori* to the recipient. In that event, the sender may transmit with its signed message a digital certificate issued by a
15 Certification Authority. The certificate is itself a signed electronic document (signed with the private key of the Certification Authority) certifying that a particular public key is the public key of the sender. A system that implements such a solution is called a Public Key Infrastructure.

Another challenge facing electronic commerce is ensuring the trustworthiness of
20 software, such as a Web browser, used by contracting parties to conduct electronic transactions. Because these transactions take place over a computer network such as the Internet, a transacting party's Web browser may be exposed to viruses, trojans and other malicious programs. Such programs may corrupt the browser and may destroy the confidence of the parties that an electronic transaction will be carried out according to their
25 intentions. For example, if a buying party's browser is corrupt, then the buying party can not be assured that the buying party's signature will not be affixed to a transaction that the buying party did not know of, did not authorize, or whose contents have been altered without the buying party's knowledge. And a selling party can not be assured that a completed transaction will not later be refuted by the buying party. A corrupt browser may
30 thus compromise the ability of the parties to conduct secure electronic commerce.

SUMMARY OF THE INVENTION

A system and method are disclosed for providing trusted browser verification. In a preferred embodiment, this verification is provided within the context of a four-corner trust
35 model. The four-corner model comprises a buyer, also referred to as the subscribing

customer, and a seller, also referred to as the relying customer, who engage in an on-line transaction.

In a preferred embodiment, the buyer is a customer of a first financial institution, referred to as an issuing participant. The issuing participant acts as a Certification Authority
5 for the buyer and issues the buyer a hardware token for the buyer's private key and a digital certificate of the buyer's public key signed by the issuing participant. Preferably, the buyer is provided with a Web browser to communicate with the sellers' Web site and conduct electronic transactions.

In a preferred embodiment, the seller is a customer of a second financial institution,
10 referred to as the relying participant. The relying participant acts as a Certification Authority for the seller and issues the seller a hardware token for the seller's private key and a digital certificate signed by the relying participant. The system also includes a root Certification Authority that issues digital certificates to the issuing and relying participants.

In a preferred embodiment, the present system and method also comprises a trusted
15 verifier. The trusted verifier ensures in a verifiable manner that the browser used by the buyer does not contain any code that is not trusted. The trusted verifier determines the status of the buyer's browser by verifying the digital signatures on each running browser component and ensuring that the signature was applied by an entity that is authorized to certify the trustworthiness of the component. In addition, the trusted verifier may compare a
20 hash of the running browser components to known-good hashes for those components.

In a preferred embodiment, the status of the buyer's browser may be either good, bad, or unknown. If the browser status is good, then all code running in the browser environment is trusted. If the browser status is bad, then the browser contains code that can not be trusted. If the browser status is unknown, then it can not be determined whether or
25 not the browser contains any code that can not be trusted.

Because the trusted verifier ensures that the buyer's browser may be trusted, the buyer may be assured that the buyer's signature will not be affixed to an electronic transaction that the buyer did not know of, did not authorize, or whose contents have been altered without the buyer's knowledge. In addition, the seller may be assured that a signed
30 electronic transaction will not later be refuted by the buyer. Thus, the trusted verifier enhances the ability of the contracting parties to conduct secure electronic commerce in the present system.

The features and advantages described in the specification are not all inclusive, and many additional features and advantages will be apparent to one of ordinary skill in the art
35 in view of the drawings, specification, and claims hereof.

BRIEF DESCRIPTION OF THE DRAWINGS

The above summary of the invention will be better understood when taken in conjunction with the following detailed description and accompanying drawings, in which:

- FIG. 1 is a block diagram of a preferred embodiment of the four-corner model employed by the present system;
- FIG. 2 schematically illustrates a first preferred embodiment of the present system that employs a distinct trusted verifier entity;
- FIG. 3 schematically illustrates a second preferred embodiment of the present system that also employs a distinct trusted verifier entity;
- FIG. 4 schematically illustrates the components preferably provided at each entity in the four-corner model;
- FIG. 5 is a block diagram of a preferred embodiment of a transaction coordinator adapted to provide a trusted browser verification service;
- FIG. 6 schematically illustrates the components preferably provided at each system entity in the preferred embodiments that employ a distinct trusted verifier entity;
- FIG. 7 is a composite block/flow diagram of a preferred embodiment in which the trusted verifier is a distinct entity;
- FIG. 8 illustrates the digitally signed content including authenticated or signed attributes in three preferred embodiments of the present invention;
- FIG. 9 illustrates one preferred embodiment of a rule set for determining the value of a browser status response;
- FIG. 10 illustrates a second preferred embodiment of a rule set for determining the value of a browser status response;
- FIG. 11 is a composite block/flow diagram of a second preferred embodiment in which the trusted verifier is a distinct entity; and
- FIG. 12 is a composite block/flow diagram illustrating a preferred embodiment in which the trusted verifier is incorporated in a participant's transaction coordinator.

DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENTS

- The present disclosure relates to a system and method for providing trusted browser verification. In a preferred embodiment, this verification is provided within the context of a four-corner trust model. A preferred embodiment of the four-corner model is shown in FIG. 1.

As shown in FIG. 1, the four-corner model preferably comprises a first institution 102 and a second institution 104. First institution 102 is referred to as the “issuing

participant” because it is a participant in the present system and it issues smart cards to its customers, as described below. Second institution 104 is referred to as the “relying participant” because it is a participant in the present system and it enables its customers to rely on representations made by issuing participant 102 and issuing participant 102's
5 customers, as described below. Participants 102, 104 may preferably be banks or other financial institutions.

Also shown in FIG. 1 are a first customer 106 and a second customer 108. First customer 106 and second customer 108 are preferably customers of issuing participant 102 and relying participant 104, respectively. First customer 106 is referred to as the
10 “subscribing customer” because this customer subscribes to services provided by issuing participant 102. First customer 106 is also referred to as the “buyer” because it typically fills that role in transactions with second customer 108, as described below.

Second customer 108 is referred to as the “relying customer” because it relies on representations made by both issuing participant 102 and subscribing customer 106. Second
15 customer 108 is also referred to as the “seller” because it typically fills that role in transactions with first customer 106, as described below. It should be recognized, however, that although the description below may speak in terms of a buyer 106 and a seller 108, first customer 106 and second customer 108 may instead have different roles in a given transaction. For example, first customer 106 may be a borrower repaying a loan to second
20 customer 108. In fact, the transaction may be any electronic communication or assertion by subscribing customer 106 to relying customer 108 that relying customer 108 needs to rely upon and trust.

Also shown in FIG. 1 is a root entity 110. Root entity 110 is typically an organization that establishes and enforces a common set of operating rules for facilitating
25 electronic commerce and electronic communications. Root entity 110 may be owned jointly by a plurality of banks and/or other financial institutions that have agreed to adhere to these operating rules. Exemplary embodiments of such a root entity are described in copending application serial No. 09/502,450, filed February 11, 2000, entitled System and Method for Providing Certification Related and Other Services and in copending application serial No.
30 09/657,623, filed September 8, 2000, entitled System and Method for Providing Certificate-Related and Other Services, which are hereby incorporated by reference.

In a preferred embodiment, the system of FIG. 1 also comprises one or more trusted verifiers shown in FIG. 1 as part of participants 102, 104. As discussed below, the trusted verifier ensures the trustworthiness of Web browsers used by customers 106, 108. The
35 trustworthiness of a customer's Web browser may be compromised by viruses or other

means. The trusted verifier allows relying parties to determine the verifiable trustworthiness of a browser.

In some preferred embodiments, each participant may serve as a trusted verifier 201 as shown in FIG. 1. These embodiments will be referred to herein as participant-verifier
5 embodiments. In other preferred embodiments, trusted verifier 201 may be a separate entity as shown in FIG. 2. These embodiments will be referred to herein as distinct-verifier embodiments. In a preferred distinct-verifier embodiment, customers may seek services directly from trusted verifier 201, as shown in FIG. 2, and as described in more detail below. Alternatively, customers may seek services from trusted verifier 201 via a
10 participant 102, 104 as shown in FIG. 3.

FIG. 4 schematically illustrates the components preferably provided at each entity in the present system. As shown in FIG. 4, participants 102, 104, and root entity 110 are each preferably provided with a transaction coordinator 202 that serves as a gateway for transmitting and receiving all inter-entity messages related to services provided by the
15 present system. Each transaction coordinator 202 is preferably provided with an associated hardware security module (HSM) 218 for signing and verifying messages. Transaction coordinators 202 provide a single interface to issuing participant 102's and relying participant 104's on-line services and implement safeguards necessary to ensure secure electronic communications between transaction coordinators 202 and other entities in the
20 four-corner model, as described in copending United States patent application serial No. 09/657,605, filed on September 8, 2000, entitled System and Method for Providing Certificate Validation and Other Services, which is hereby incorporated by reference.

Participants 102, 104, and root entity 110 are each further preferably provided with an Online Certificate Status Protocol (OCSP) responder 204 and associated HSM 206 for
25 signing certificate status responses and verifying signatures on certificate status requests. In addition, each participant 102, 104 and root entity 110 is further preferably provided with a billing database 208 (connected to a bank billing application 210 in the case of participants 102, 104), a raw transaction log 212, a customer database 214, a risk manager 216 (connected to customer database 214), and a hardware security module 218, each of which
30 is connected to transaction coordinator 202. Each of these components is more fully described in the above-cited application serial No. 09/657,605.

FIG. 5 illustrates a preferred embodiment of a transaction coordinator incorporating a trusted browser verification service 318. Transaction coordinator 202 preferably comprises an interface 302 comprising two components: a TC request manager 304 and a
35 transport services component 306. Interface 302 passes communications to and from a

plurality of service modules 308 and core components 310. Service modules 308 preferably include a trusted browser verification service 318. The interface components, the core components, and the other service modules shown in FIG. 5 are described in the above-cited application, serial No. 09/657,605.

5 Each participant is also preferably provided with a trusted browser verification component 219 and a trusted component database 221, as shown in FIG. 4. Transaction coordinator 202 is configured to transmit and receive messages from trusted browser verification component 219. Trusted browser verification component 219 comprises code that is adapted to create hashes, compare hashes, sign hashes, verify signatures, store
10 signatures, retrieve signatures, send and receive signatures, and generate a report on the status of a browser. These functions may be accomplished in part by using functionality of the underlying browser, the operating system, or other cryptographic libraries and modules.

Each participant is also preferably provided with a trusted component database 221 for storing hashes, as shown in FIG. 4. In a preferred embodiment, trusted component
15 database 221 stores, for each browser component used by one or more subscribing customers, the identities and digital certificates of those entities authorized to certify the integrity of the browser component. Trusted component database 221 may also preferably store known-good hashes for each such browser component, as described below.

In a preferred distinct-verifier embodiment, trusted browser verification is preferably
20 provided by a trusted browser verifier entity 201. Accordingly, that entity is preferably provided with a trusted browser verification component 230 and a trusted component database 232. FIG. 6 schematically illustrates the components preferably provided at each entity in a preferred distinct-verifier embodiment.

As further shown in FIGs. 4 and 6, relying customer 108 is preferably provided with
25 a Web server 220 adapted to receive and transmit information via the Internet. Relying customer 108 is further preferably provided with a bank interface 222 for accessing system services, as described in more detail below. An exemplary bank interface is described in copending application serial No. 09/657,604, filed on September 8, 2000, entitled System and Method for Facilitating Access by Sellers to Certificate-Related and Other Services.
30 Relying customer 108 is preferably further provided with a hardware security module 250 for signing and verifying signatures on messages. Relying customer 108 is preferably further provided with a trusted browser verification component 251 and a trusted component database 252.

In a preferred embodiment, subscribing customer 106 is preferably provided with a
35 trusted browser verification component 227. Trusted browser verification component 227

comprises code that is adapted to create hashes, compare hashes, sign hashes, verify signatures, store signatures, retrieve signatures, send and retrieve signatures, and generate a report on the status of a browser. Trusted browser verification component 227 may generate a hash from a copy of a browser and any browser components actually running on the buyer's computer at the time the hash is made. Alternatively, the hash may be generated from a copy of the browser and any browser components stored in non-volatile memory at the buyer's computer, for example stored on the buyer's hard drive. Such hash may be generated and stored when an applet is downloaded or when the browser is launched and the plug-ins are loaded.

Preferably, the software for implementing trusted browser verification as described herein may be distributed to customers in a number of different ways. First, root entity 110 may distribute the software to browser manufacturers or permit browser manufacturers to create software for implementing the functionality described herein. These manufacturers may incorporate this software into a browser for distribution to customers. Second, trusted verifier 201 may distribute appropriate code to customers as a plug-in or as a library for their browsers. Third, trusted verifier 201 may distribute appropriate code as an applet that customers may download.

As further shown in FIG. 4, subscribing customer 106 is further preferably provided with a Web browser 224 adapted to receive and transmit information via the Internet.

Subscribing customer 106 preferably receives Web browser 224 from trusted verifier 201 or other sources. If subscribing customer 106 receives Web browser 224 from trusted verifier 201, the code that comprises Web browser 224 is preferably signed by trusted verifier 201. If subscribing customer 201 receives Web browser 224 from another source, the browser code may or may not be signed.

Subscribing customer 106 may also receive other browser components, such as plug-ins or applets, and other components, such as proxies, from trusted verifier 201 or other sources. Some or all of these other browser components may be signed by the manufacturer or another entity. Others of such components may be unsigned.

Subscribing customer 106 preferably stores the digital signatures for all browser components that it receives in a trusted component database 228. Trusted component database 228 may also be used to store known-good hashes of these components, as described below.

In a preferred embodiment, each system entity is preferably provided with a smart card for signing messages. In addition, each system entity is further preferably provided

35

with two digital certificates (with corresponding private keys) to facilitate authentication: an identity certificate and a utility certificate.

5 The identity private key is used to produce digital signatures that are required as evidence of an entity's contractual commitment to the contents of an electronic transaction, such as a purchase order.

The utility private key is used to produce digital signatures that allow additional transactional security via actions like, data encryption, key encryptions and exchange, establishment of encrypted channels with communicating parties via Secure Sockets Layer/Transport Layer Security (SSL/TLS), and for Internet Protocol Security (IPSec)
10 authentication. Typically, utility certificates are used to support secure socket layer sessions, to encrypt S/MIME messages, and for other utility applications. Any reference in this document to the term "certificate" refers to an identity certificate unless otherwise stated.

Having described the system architecture and components, preferred embodiments
15 for providing trusted browser verification are now described.

Trusted browser verification may be implemented in a number of ways. In a first preferred distinct-verifier embodiment, relying customer 108 may look to relying participant 104 to process a browser status request regarding Web browser 224. In this embodiment, relying participant 104 forwards the browser status request to trusted verifier 201 and
20 returns to relying customer 108 a browser status response from trusted verifier 201.

Relying customer 108 may include its browser status request as part of a certificate validation request for subscribing customer 106's certificate or transmit it as a separate request. If relying customer 108 bundles the browser status request with a certificate validation request, then transaction coordinator 202_{RP} preferably forwards the browser status
25 request to trusted verifier 201 and processes itself the certificate validation request as described in copending United States patent application serial No. 09/657,605, filed on September 8, 2000, entitled System and Method for Providing Certificate Validation and Other Services.

In a second preferred distinct-verifier embodiment, relying customer 108 may send a
30 browser status request directly to trusted verifier 201. Trusted verifier 201 checks the status of Web browser 224 and returns a browser status response directly to relying customer 106.

In a preferred participant-verifier embodiment, relying participant 104 may process a browser status request using transaction coordinator 202_{RP} and a trusted browser verification component 219_{RP} maintained at relying participant 104.

35

In other preferred embodiments, browser status requests may be received from, and responses to those requests may be sent to, subscribing customer 106.

In still other preferred embodiments, instead of transmitting browser status requests to trusted verifier 201, customers 106, 108 may receive a known-good set of hashes from trusted verifier 201 or trusted browser verification component 219. Customers 106, 108 may then compare these known-good hashes to those of buyer's browser components to verify their integrity.

Preferred operation of these embodiments is described below.

FIG. 7 schematically illustrates trusted browser verification in a preferred distinct-verifier embodiment. In step 701, relying customer 108 sends subscribing customer 106 a purchase order. In step 702, Web browser 224 invokes a signing interface that sends the purchase order to smart card 226 for signature. A suitable signing interface is described in copending provisional patent application serial No. 60/224,994, filed August 14, 2000, entitled Signing Interface Requirements, Smart Card Compliance Requirements, Warranty Service Functional Requirements, and Additional Disclosure, which is hereby incorporated by reference.

In step 703, the purchase order is signed. In a preferred embodiment, when the signature is a PKCS #7 signature, the digital signatures of all signed components running in the buyer's browser environment are retrieved from trusted component database 228 and included as authenticated attributes in the PKCS #7 signature. Alternatively, when the signature is an XML digital signature, the digital signatures of all signed components running in the browser environment are included in the XMLDSIG as signed attributes.

In a further preferred embodiment, any unsigned code running in the browser environment is preferably included as an authenticated or signed attribute in the buyer's digital signature. This code may preferably be copied from RAM (i.e., the particular instance of the unsigned code currently running). Alternatively, it may be copied from non-volatile memory at the buyer's computer, such as the buyer's hard drive.

In a further preferred embodiment, trusted browser verification component 227 hashes the code of all signed browser components actually running at the time the purchase order is signed. The code for these signed browser components may preferably be retrieved from RAM (i.e., the actual instance of the signed browser components currently running). Alternatively, this code may be retrieved from non-volatile memory at the buyer's computer, such as the buyer's hard drive. A hash of each such component is then created, and included as an authenticated or signed attribute in the digital signature created in step 703.

FIG. 8 summarizes the digitally signed content including authenticated or signed attributes in each of the three preferred embodiments described above for step 703. In particular, as shown in FIG. 8, in the first preferred embodiment described above, the buyer's digital signature is executed on:

- 5 (1) the purchase order; and
- (2) the digital signature of each signed component running in the browser environment.

By contrast, in the first further preferred embodiment described above, the buyer's digital signature is executed on:

- 10 (1) the purchase order;
- (2) the digital signature of each signed component running in the browser environment; and
- (3) any unsigned code running in the browser environment.

By contrast, in the second further preferred embodiment described above, the buyer's digital signature is executed on:

- 15 (1) the purchase order;
- (2) the digital signature of each signed component running in the browser environment;
- (3) any unsigned code running in the browser environment; and
- 20 (4) the code of each signed component running in the browser environment.

In step 704, subscribing customer 106 sends the signed purchase order (including its authenticated or signed attributes) to relying customer 108. In step 705, relying customer 108 receives the signed purchase order and authenticates the subscribing customer's signature using the subscribing customer's certificate. If the second further preferred embodiment described above is implemented, the relying customer also compares the hashes created by subscribing customer 106 for all digitally signed components to the hashes in the digital signatures of those components for an added degree of security that the code actually running or stored in non-volatile memory on the buyer's computer is in fact the code verified by the trusted entity's signature.

- 30 In step 706, trusted browser verification component 251 of relying customer 108 extracts from the signed purchase order the digital signatures of all signed components running on the subscribing customer's browser and generates a browser status request for these components. The buyer's signature on the unsigned code may also preferably be included in this request, if the first further preferred embodiment described above is
- 35 implemented.

In step 707, relying customer 108 signs the browser status request and sends it to relying participant 104 via bank interface 222. As noted above, relying customer 108 may bundle the browser status request with a certificate validation request for subscribing customer 106's certificate. If a certificate validation request is bundled with the browser status request, then transaction coordinator 202 preferably processes the certificate validation request as described in copending United States patent application serial No. 09/657,605, filed on September 8, 2000 entitled System and Method for Providing Certificate Validation and Other Services. In step 708, transaction coordinator 202_{RP} forwards the browser status request to trusted verifier 201.

10 In step 709, for each browser component included in the browser status request, trusted verifier 201 identifies the entity that signed the digital signature and verifies the authenticity of that digital signature, using, for example, the signer's certificate. In addition, trusted verifier 201 may validate the entities certificate, if desired.

In step 710, trusted verifier 201 retrieves from trusted component database 232 the
15 identities of those entities authorized to certify the trustworthiness of each browser component in the browser status request. It then determines whether the entity that executed the digital signature on each signed component is authorized to do so. For example, if the component is the Netscape Communicator™ browser, Netscape™ (i.e., the entity that created the component) may be designated a trusted entity to certify the integrity
20 of this component. Similarly, if the component was a Microsoft™ applet downloaded by the user, Microsoft™ might be designated a trusted entity to certify the integrity of this component. Alternatively or in addition, issuing participant 102 may be designated a trusted entity authorized to certify browser components running on its customers' computers (e.g., subscribing customer 106). Alternatively or in addition, another system entity, such as
25 trusted verifier 201, may be designated a trusted entity to certify the integrity of one or more browser components.

In addition, if desired, all customers 106 may be identified as authorized to certify otherwise unsigned code running on their computers. Alternatively, these customers may be required to pre-register otherwise unsigned code with trusted verifier 201 by signing the
30 code and formally assuming responsibility for its trustworthiness.

In a preferred embodiment, known-good hashes of browser components to be verified are available to trusted verifier 201. Trusted verifier may store these known-good hashes in its trusted component database 232 or alternatively may obtain these known-good hashes on an "as needed" basis from the entity that executed the digital signature certifying
35 the component when a request to verify the component is received. In this preferred

embodiment, as shown in step 711, trusted verifier 201 retrieves or obtains a known-good hash of each browser component to be verified, and compares it to the hash contained in the digital signature for that component included in the browser status request.

In step 712, trusted verifier 201 generates a browser status response. In a preferred embodiment, this response may take on one of three values: (1) GOOD; (2) BAD; or (3) UNKNOWN. FIG. 9 demonstrates one preferred embodiment for determining the value of a browser status response depending on the results of steps 710-711. In particular, as shown in FIG. 9, in this preferred embodiment, if the hash of any browser component does not match the known-good hash stored by trusted verifier 201, then the browser status response returns BAD. If, however, the hash matches the stored known-good hash, but the entity that executed the digital signature either can not be determined or is not authorized to certify the trustworthiness of the browser component, then the browser status response returns UNKNOWN. Finally, if the hash matches the stored known-good hash and the entity that executed the digital signature is authorized to certify the trustworthiness of the browser component, then the browser status response returns GOOD.

As will be recognized, other alternative rule sets for determining whether a browser status response should return GOOD, BAD, or UNKNOWN may be employed. One alternative rule set for determining browser status responses is illustrated in FIG. 10. Preferably, the rule set for making these determinations is determined according to the trust model employed by the system and selected by a policy management authority for the system.

In step 713, trusted verifier 201 signs the browser status response and transmits it to transaction coordinator 202_{RP}. In step 714, transaction coordinator 202_{RP} forwards the browser status response to relying customer 108.

In step 715, relying customer 108 verifies trusted verifier 201's signature on the hash response (using, e.g., its certificate). In addition, relying customer 108 may validate trusted verifier 201's certificate, if desired. In step 716, relying customer 108 reviews the status report generated by trusted verifier 201. The final decision on whether or not to use the information on the status of Web browser 224 and in what manner preferably rests with relying customer 108. Alternatively, relying customer 108 may be required to act in a particular manner (e.g., disaffirming a transaction) depending on the browser status response (e.g., if the response is BAD). Such requirements may, for example, be specified in system operating rules, such as those described in the above-cited application serial no. 09/657,623. In step 717, relying customer 108 sends a message to subscribing customer 106 either confirming or disaffirming the transaction.

In a second preferred distinct-verifier embodiment, relying customer 108 may instead send the browser status request directly to trusted verifier 201, as indicated at step 707a. Trusted verifier 201 preferably performs trusted browser verification as described above. In step 713a, trusted verifier 201 generates a report on the trusted status of Web browser 224 and sends the status report to relying customer 108. Relying customer 108 reviews the status report generated by trusted verifier 201. In step 717a, relying customer 108 sends a message to subscribing customer 106 either confirming or disaffirming the transaction. In alternative versions of these embodiments, the status requester may be subscribing customer 106, which may transmit the browser status request to trusted verifier 201 either directly or via its issuing participant 102.

FIG. 11 schematically illustrates trusted browser verification in a third preferred distinct-verifier embodiment. In step 1101, relying customer 108 sends subscribing customer 106 a purchase order. In step 1102, Web browser 224 invokes a signing interface that sends the purchase order to smart card 226 for signature.

In step 1103, the purchase order is signed. As noted above, the executed digital signature preferably comprises authenticated or signed attributes that include all digital signatures of components running in the browser environment and may include additional authenticated or signed attributes as described in the first and second further preferred embodiments.

In step 1104, subscribing customer 106 transmits a hash request to trusted verifier 201 requesting a set of known-good hashes corresponding to the browser components running in its browser environment. In step 1105, trusted verifier 201 retrieves the known-good hashes for those components and includes them in a signed hash response to subscribing customer 106.

In step 1106, subscribing customer 106 sends the signed purchase order and the hash response to relying customer 108. In step 1107, relying customer 108 verifies trusted verifier 201's signature on the hash response (using, e.g., its certificate). In addition, relying customer 108 may also validate trusted verifier 201's certificate, if desired. In step 1108, relying customer 108 compares the known-good hashes in the hash response to those of the components running in the buyer's browser environment to confirm the status of Web browser 224. In step 1109, relying customer 108 sends a message to subscribing customer 106 either confirming or disaffirming the transaction.

In a fourth preferred distinct-verifier embodiment, the hash request and/or hash response may be exchanged between relying customer 108 and trusted verifier 201.

FIG. 12 schematically illustrates trusted browser verification in a preferred participant-verifier embodiment. In step 1201, relying customer 108 sends subscribing customer 106 a purchase order. In step 1202, Web browser 224 invokes a signing interface that sends the purchase order to smart card 226 for signature.

5 In step 1203, the purchase order is signed. As noted above, the executed digital signature preferably comprises authenticated or signed attributes that include all digital signatures of components running in the browser environment and may include additional authenticated or signed attributes as described in the first and second further preferred embodiments.

10 In step 1204, subscribing customer 106 sends the signed purchase order (including its authenticated or signed attributes) to relying customer 108. In step 1205, relying customer 108 receives the signed purchase order and authenticates the subscribing customer's signature using the subscribing customer's certificate. If the second further preferred embodiment described above is implemented, the relying customer also compares
15 the hashes created by subscribing customer 106 for all digitally signed components to the hashes in the digital signatures of those components for an added degree of security that the code actually running or stored on the buyer's computer is in fact the code verified by the trusted entity's signature.

In step 1206, trusted browser verification component 251 of relying customer 108
20 extracts from the signed purchase order the digital signatures of all signed components running on the subscribing customer's browser and generates a browser status request for these components. The buyer's signature on the unsigned code may also preferably be included in this request, if the first further preferred embodiment described above is implemented.

25 In step 1207, relying customer 108 signs the browser status request and sends it to relying participant 104 via bank interface 222. As noted above, relying customer 108 may bundle the browser status request with a certificate validation request for subscribing customer 106's certificate. In step 1208, relying participant 104 forwards the request to issuing participant 102.

30 In step 1209, for each browser component included in the browser status request, issuing participant 102 identifies the entity that signed the digital signature and verifies that digital signature, using, for example, the signer's certificate.

In step 1210, issuing participant 102 retrieves from trusted component database 232 the identities of those entities authorized to certify the trustworthiness of each browser

35

component in the browser status request. It then determines whether the entity that executed the digital signature on each signed component is authorized to do so.

In a preferred embodiment, in step 1211, issuing participant 102 retrieves or obtains a known-good hash of each browser component to be verified, and compares it to the hash
5 contained in the digital signature for that component included in the browser status request.

In step 1212, issuing participant 102 generates a browser status response. In step 1213, issuing participant 102 signs the browser status response and transmits it to transaction coordinator 202_{RP} of relying participant 108. In step 1214, transaction coordinator 202_{RP} signs and forwards the browser status response to relying customer 108.

10 In step 1215, relying customer 108 verifies the signatures on the browser status response (using, e.g., the certificates of participants 102, 104). In addition, relying customer 108 may validate those certificates, if desired. In step 1216, relying customer 108 reviews the status report generated by issuing participant. In step 1217, relying customer 108 sends a message to subscribing customer 106 either confirming or disaffirming the transaction.

15 While the invention has been described in conjunction with specific embodiments, it is evident that numerous alternatives, modifications, and variations will be apparent to those skilled in the art in light of the foregoing description.

20

25

30

35